学校编码：10384　　分类号_____密级_____
学　　号：200430040　　UDC_____

硕　士　学　位　论　文

# 无线 Mesh 网络中安全路由协议的研究

# Research of Secure Routing Protocol in Wireless Mesh Network

喻继燊

指导教师姓名：肖明波　　教授
专　业　名　称：信号与信息处理
论文提交日期：2007 年 10 月
论文答辩时间：2007 年 10 月
学位授予日期：2007 年　　月

答辩委员会主席：_____
评　　阅　　人：_____

2007 年 10 月

# 厦门大学学位论文原创性声明

兹呈交的学位论文，是本人在导师指导下独立完成的研究成果。本人在论文写作中参考的其他个人或集体的研究成果，均在文中以明确方式标明。本人依法享有和承担由此论文产生的权利和责任。

声明人（签名）：

年　月　日

# 厦门大学学位论文著作权使用声明

本人完全了解厦门大学有关保留、使用学位论文的规定。厦门大学有权保留并向国家主管部门或其指定机构送交论文的纸质版和电子版，有权将学位论文用于非赢利目的的少量复制并允许论文进入学校图书馆被查阅，有权将学位论文的内容编入有关数据库进行检索，有权将学位论文的标题和摘要汇编出版。保密的学位论文在解密后适用本规定。

本学位论文属于

1.保密（），在年解密后适用本授权书。

2.不保密（　）

（请在以上相应括号内打“√”）

作者签名：　　日期：　　年　　月　　日

导师签名：　　日期：　　年　　月　　日

# 摘 要

随着无线局域网（WLAN）和 3G 网络的普及，无线通信技术已经在生活中无处不在了。所以如何为用户在更大的覆盖范围内提供高的速率已经成了下一代无线通信技术的主要需求。无线 Mesh 网络(Wireless Mesh Network)简称 WMN，做为一种新型的无线通信网络，有着自组织性、自愈性、频谱效率高、覆盖范围大、可扩展性强、可靠性强等众多无可比拟的优势，在很大程度上满足了这一技术需求。所以我们可以肯定，WMN 将成为下一代无线通信技术的重要组成部分。

无线 Mesh 网的发展起源于无线 Ad hoc 网的研究，将无线 Ad hoc 网的特点应用于 Internet 的接入；在其分布式网路的特点上加入了更灵活的选择节点功能的特性。因此与无线 Ad hoc 网络一样，高效、安全的路由机制是保证网络正常工作的一个重要因素。但是就目前来说，对 WMN 路由的研究还较少，而且主要集中在提高协议性能上，路由协议安全的研究更是寥寥无几。

因此本文重点研究无线 Mesh 网的安全路由机制。首先介绍了 WMN 的结构、特点以及关键技术；随后介绍了两种较成熟的分布式无线网络的路由协议——DSR 和 AODV，并对其性能进行了对比，随后又介绍在这两种路由协议下的几种安全路由机制，重点介绍了一种无线 Ad hoc 下鉴别的安全路由机协议——ARAN 协议；随后分析了 WMN 的路由安全隐患以及安全路由的设计特点；最后提出了一种基于 ARAN 协议鉴别思想的 WMN 安全路由机制——ARWMN 协议，并对其安全性能进行了分析。

关键词：WMN，无线 Ad hoc 网络，安全路由，ARAN 协议

# Abstract

With the rapid growth of WLANs and 3G networks, wireless communication technologies are penetrating our life. As a result, how to provide wider wireless coverage with higher data rate, becomes the major demand of the next-generation wireless systems.

As a newly developed wireless network, Wireless Mesh Network (WMN) characterized by distinguished features such as self-organization, self-healing, high spectral efficiency, wide coverage, high scalability, and high reliability, meets such a challeng in many ways. We are certain that WMN will be an important component in next-generation wireless system.

WMN originates from the Ad Hoc network, and retains it's flexibility in choosing routes, while introducing many features of the Internet.Therefore, like the Ad Hoc network, it is very important to have an effective and secure routing mechanism to ensure successful operation of WMN. However, there are few results on the routing of WMN, most of which focus on improving performance of the protocols, and even less on the secure routing of WMN.

In this work, we mainly study the scure routing of WMN. The architecture, feature, and key technologies of WMN are introduced first. Then, two well-known routing schemes for Ad Hoc networks, DSR and AODV, are discussed. Some secure routing mechanisms under these two schemes are presented, with emphasis on the authenticated routing of Ad Hoc network (ARAN). By analyzing the possible threats and characteristic of WMN, we propose ARWMN, an improved secure routing of WMN based on ARAN. Its performance is evaluated.

Keywords: WMN; Ad hoc; Secure Routing; ARAN.

# 目 录

# Contents

# 第一章 绪论

## 1.1 引言

WMN[1] (Wireless Mesh Network ，无线 Mesh 网络)是一种多跳、具有自组织和自愈特点的宽带无线网络结构，即一种高容量、高速率的分布式网络。它以探索无线移动通信与 IP 技术的结合为宗旨，研究在小型区域范围内实现允许多个网络同时存在、不同网络自动区分、拓扑结构动态可变、具有多跳和动态路由能力的自组织网络结构形式。它又被称为无线网状网络或无线网格网络。

在网络拓扑上，WMN 与移动 Ad hoc 网络相似，但网络的大多数节点基本静止不移动，不用电池作为动力，拓扑变化较小；在单跳接入上，WMN 也可以看成是一种特殊的 WLAN。作为一种新型网络结构形态，WMN 结构已经被纳入到 802.16，802.16e，802.11s 等标准中。WMN 作为未来无线城域核心网最理想的方式之一，极有可能挑战 3G 技术，是构建 B3G/4G 的潜在技术之一。WMN 作为一种新型的应用网络，因其自身特点以及在家庭、企业和公共场所等诸多领域的广阔的应用前景，所以具有重要的理论意义和实际意义。

## 1.2 WMN 的历史背景

美国早在 80 年代初即提出了自组织网络的概念，目前其研究重点在移动 Ad Hoc 网络(MANET)。我国从七五后期开始自组织网络技术研究。无线网络技术是当前获得迅速发展的技术，它允许移动用户采用更加灵活方便的方式接入网络。典型的无线网络(Wireless LAN)WLAN 通常具有两种组织形式:中心结构网络(Infrastructure network)和 Ad Hoc 网络(Infrastructure less network)。中心结构网络由包含固定有线网关的网络组成。在无线覆盖范围内，移动主机与基站(固定有线网关)进行通信，并可在通信过程中移动。当移动主机离开原基站的无线覆盖范围后，它可与另一个基站建立连接并通过该基站继续进行通信。在这种组网和通信方式中，基站位置是固定不动的。GSM 系统即是采用这种网络组织形式。Ad Hoc 网络是无线网络的另一种组织方法。在 Ad Hoc 网络中，所有节点

都处于平等地位，它们之间都可能有通信关系存在，同时每个节点还承担着组网和为其它节点中继的义务。网络中的所有节点都像路由器一样参与路由的发现和维护。但是移动 Ad hoc 网络由于其应用环境和技术成本等原因，不适合直接应用到民用通信领域，而在通信领域中，最大的民用通信业务应该是包括 VoIP 业务在内的因特网业务。而民用通信用户的移动性行为也远低于军事通信用户，所以为了能够实现无线通信中的无处不在的(Ubiquitous)通信目标，我们需要基于移动 Ad hoc 网络的技术基础，开发出一种完全适用于民用通信的无线多跳网络技术。于是 WMN 技术就随着这一需求孕育而生了。

在单跳网络上，WMN 可以看成是一种特殊的 WLAN，除移动性较低外，WMN 本质上是一种 Ad hoc 网络。目前主要观点认为，WMN 是一种由无线链路连接路由器和终端设备的静态无线网络，是 Internet 的无线版本。作为一种新型网络结构形态，Mesh 结构已被纳入到 802.16-2004.802.16e 和即将制定的 802.11s 标准中。

目前，国内外对 WMN 和移动 Ad Hoc 网络的研究主要在于其自组织算法和路由算法的研究。但在移动 Ad hoc 网络和 WMN 上，还没有路由协议正式标准。Mesh 路由协议基本沿用 Ad hoc 网络路由协议，但需要针对 WMN 的特点设计专门适用于 WMN 的高效路由协议。而现在几种典型的路由协议有:DSDV(目的序列距离矢量路由协议)、DSR(动态源路由协议)、TORA(临时按需路由算法)和 AODV(Ad hoc 按需距离矢量路由协议)等。

## 1.3 WMN 的体系结构及其特点

WMN 与传统意义上的移动 Ad hoc 网络结构有一定的差异。一般来说，WMN 有客户节点、Mesh 路由节点和网关节点组成。但是根据网络的具体配置的不同，WMN 不一定包含以上所有类型的节点。

按照体系结构划分，无线网状网络可以分为三种，分别为：骨干网结构（Backbone WMN），终端组网结构（Clients WMN）和混合结构（Hybrid WMN）。

### 1.3.1 骨干网结构

图 1.1 所示为 WMN 的典型骨干网结构，分为上层和下层两个部分。在这一

结构中，终端节点可以是普通 VoIP 手机、笔记本电脑和无线 PDA 等。这些终端节点设备通过 Mesh 路由器接入到上层 Mesh 结构的网络中去，实现了网络节点的互通。

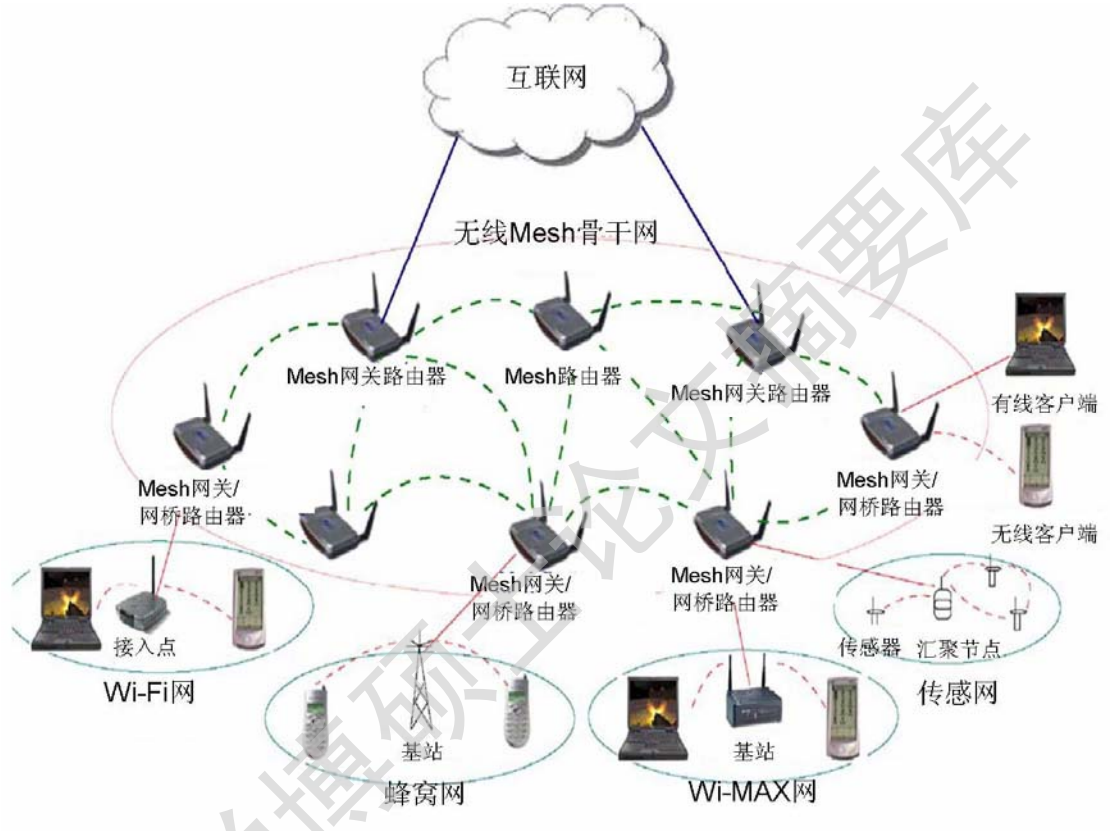


**图 1-1 骨干网 WMN 结构**

### 1.3.2 终端组网结构

如图 1-2 所示 WMN 中最简单的一种结构——终端组网结构。在此网络结构中，客户节点既是业务的使用者又是业务的提供者，即具有数据的转发功能，可以向网络中的其他节点转发它所接收到的数据包。该 WMN 吸收了星形网与网状网两种网络的优点，是对两者的一种无缝融合。具体来说，WMN 可以看作是 WLAN 和 ad hoc 网络的融合，发挥了两者的优势，而这种融合是通过在网络节点上执行 WMR(wireless mesh routing) 协议来完成的。

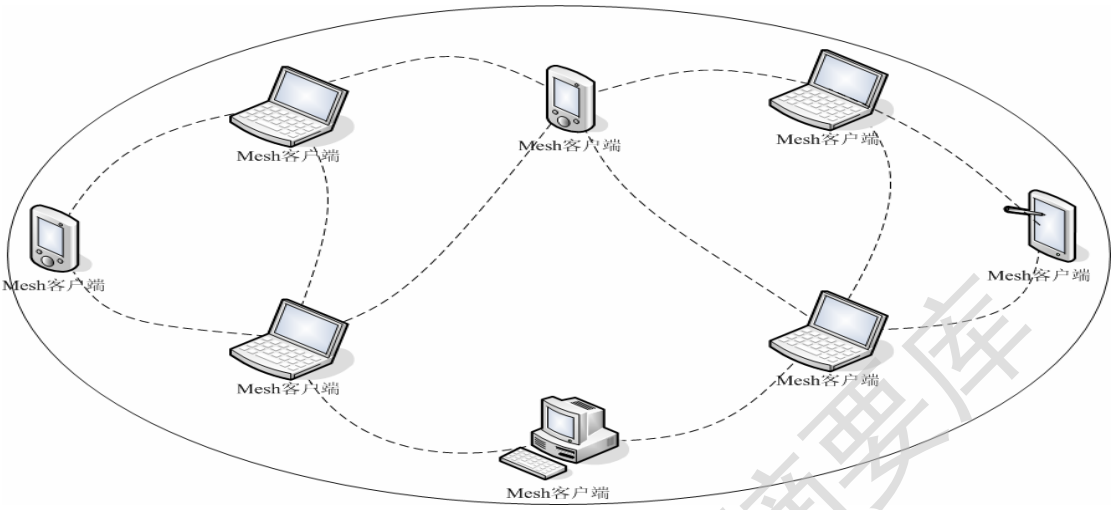


**图 1-2 终端组网 WMN 结构**

### 1.3.3 混合结构

图 1-3 所示为混合 WMN 结构，是以上两种结构的混合。在此结构中，终端节点已经不再是市场上的仅仅支持 WLAN 的普通设备，而是增加了具有转发和路由功能的 Mesh 设备，设备之间可以以 Ad hoc 方式互联，直接通信。一般来说，终端节点设备需要同时能够支持接入上层网络 Mesh 路由器和同层网络的对等节点的功能。

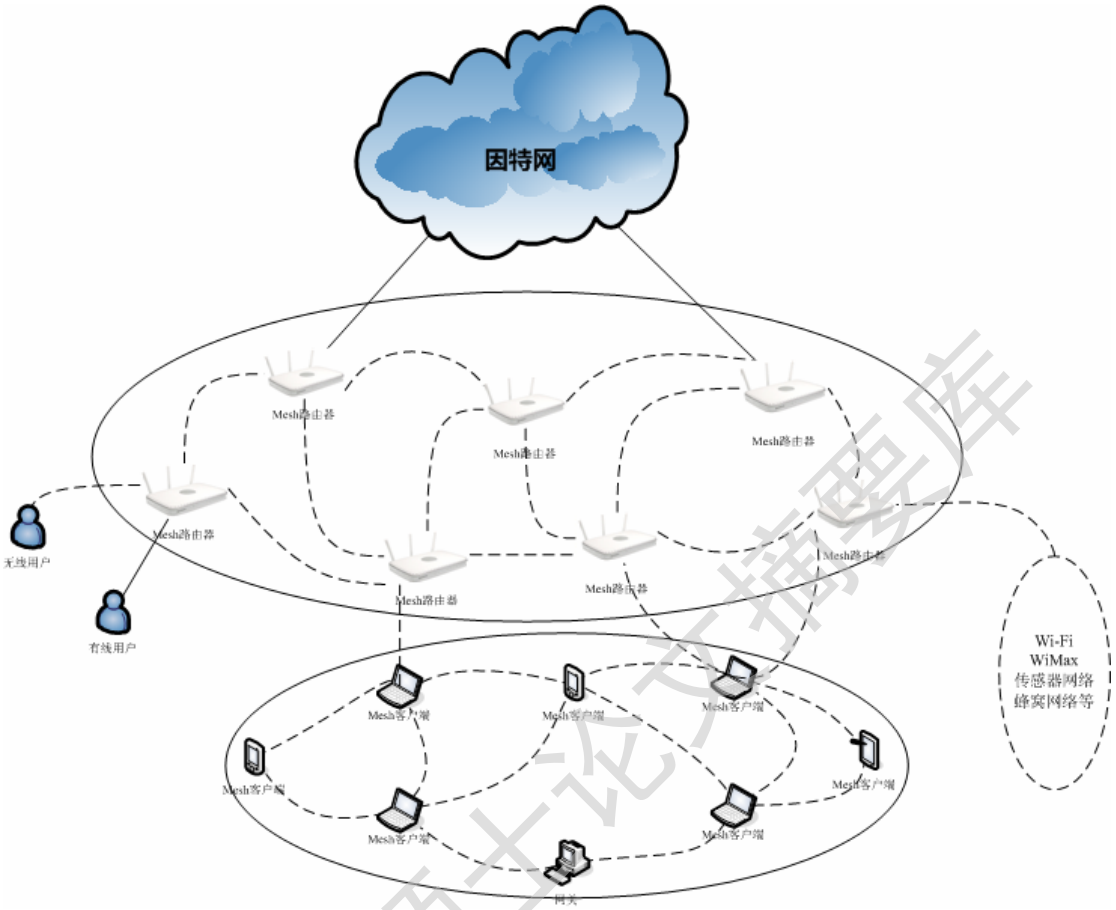


**图 1-3 混合 WMN 结构**

### 1.3.4 结构特点

WMN 具有以下一些结构上或技术上的特点：

- 自愈性：WMN 可以提供完全的端到端的多重冗余路由，这就意味着如果最近的节点出现故障或者受到干扰，数据包将自动路由到备用路径继续进行传输，整个网络的运行不会受到影响。若由于某种原因某个链路失效，网络能自动地更换路由。
- 多跳无线网络：在不牺牲当前信道容量的情况下，扩展当前无线网络的覆盖范围是 WMN 最重要的目标之一。
- 非视距连接：可以通过短距离的多跳链路，提供非视距的连接。
- 支持 Ad hoc 网络结构：具有自形成、自愈和自组织能力。
- 组网方便：WMN 灵活的网络结构便利的网络配置、容错能力和网格连通性，大大提升了现有网络的性能。在较少的前期投资下，WMN 可以根据需要逐步扩展。

- 可靠性：在 Mesh 网络结构中为了提高链路质量，可通过增加中间节点，即缩短节点之间的距离来实现。
- 支持多种网络接入：WMN 既支持 Internet 接入又支持对等通信，同时还支持使用不同通信协议网络之间的通信。
- 移动性取决于节点的类型：如前面所述，WMN 通常有几类节点，分别具有不同的移动特性。Mesh 网关和 Mesh 路由器的移动性通常较低，而 Mesh 客户终端既可以是静止的，也可以是任意的移动节点。
- 高吞吐量及高频谱利用率：由于 Mesh 的连接方式，链路变得更短，干扰也较少，所有可以提供更高吞吐量及更高频谱利用率。
- 功耗限制取决于节点类型：Mesh 路由器通常是通过有线电源进行供电，所以它对能耗的要求并不严格。而 Mesh 终端通常是通过电池供电，所以能源效率高的协议对于网络终端是非常重要的。

## 1.4 WMN 安全路由协议的研究意义

由于网络层是 WMN 与其它网络的主要区别所在，所以各科研机构目前主要致力于网络层的研究。其主要研究内容包括 WMN 中的路由问题、网际互联问题、安全问题，以及 QoS 问题等。

WMN 作为一种新型的无线移动网络，容易受到安全攻击，比如受到窃听、伪造、拒绝服务等攻击。其安全目标与传统有线网络中的安全目标是一致的，它们包括:可用性、机密性、完整性、安全认证和抗抵赖性，但两者却具有不同内涵。在传统网络中，主机之间的连接是固定的，网络采用层次化的体系结构，并具有稳定的拓扑，提供了多种服务以充分利用网络的现有资源，包括路由器服务、命名服务、目录服务等。在此基础上提出了相关的安全策略，如加密、认证、访问控制和权限管理、防火墙等等。而在 WMN 中节点之间通过无线信道相连，没有专门的路由器，由节点自身充当路由器。也没有命名服务、目录服务等网络功能。这就导致了在传统网络中的安全机制不再适用于 WMN。而且与 WLAN 的单跳机制相比，WMN 的多跳机制决定了用户通信要经过更多的节点。而数据通信经过的节点越多，安全问题就越变得不容忽视。尽管有线网络中使用的各种安全技术，如虚拟专用网（VPN）、SSL/TLS 同样可以用来解决 WMN 的安全问题。

但正如 Internet 一样，WMN 的安全也是一个不容忽视的问题。

由于 WMN 路由协议基本沿用 Ad hoc 网络路由协议，而移动 Ad hoc 网络本身存在很多安全隐患，而现今已有的路由协议基本上没有考虑安全的问题。而且相对于移动 Ad hoc 网络 WMN 有其自身的路由特点。这些特点主要包括：

(1) 拓扑变化相对稳定：由于 Mesh 路由器移动性较低，一般使用有线电源，生存周期长，拓扑结构变化较少。

(2) Mesh 路由器运算能力有限：Mesh 路由设备一般比较小巧，运算能力较差，这对使用运算量较大的安全协议有影响。

(3) 主要的路由业务为查找到网关节点的路径：这是由 WMN 的主要业务——提供来往于因特网的业务而决定的。

(4) 要针对节点类型进行区分：针对不同功能的节点，需要有更完善的判别机制。

(5) 安全等级需求较低：由于 WMN 主要用于民用业务，所传递的信息价值也相对较低，所以对于安全等级的需求也较低。

因此针对 WMN 的路由特点定制出特别适用与 WMN 的安全路由协议具有相当积极的理论意义和实际意义。

## 1.5 本文研究的目的和内容

通过研究已经较成熟的移动 Ad hoc 网络的路由协议，以及相关安全路由方案，提出一个适用于 WMN 的安全路由协议，促进 WMN 技术的发展进程。

第一章，主要介绍了 WMN 的基本情况，包括 WMN 的历史背景、结构特点及其路由协议的特点。

第二章，首先分析现有路由算法的设计思想，并详细叙述了移动 Ad hoc 网络下的两个典型的按需路由协议 AODV 和 DSR，并进行了性能比较。

第三章，首先介绍 WMN 安全方面所遇到的挑战及其安全设计的最终目的，然后分别阐述了密码学里的两种不同的加密体制——对称密码体制和公钥密码体制，并各列举其相应的算法，分析了两种体制算法的优缺点。

第四章，介绍了目前无线 Ad hoc 网络三种主要的安全路由协议：安全 Ad hoc 路由( Secure Aware ad hoc Routing，SAR) 、移动 Ad hoc 网络的安全路由协